Cryptomathic Signer PKI Plugin Guide

Revision History

Version	Date	By	Comments
1	15/01/10	Cryptomathic	Initial release of document
2	05/05/10	Cryptomathic	Added SignerCtxKey.SignerCostumerDomain

Introduction

The Cryptomathic Signer PKI Plugin is an authentication plugin for the SignOn Library framework that exposes the PKI interface through the application context to other plugins. Read the document "Sign-On projektet: A national architecture for SignOn" for details on entire SignOn Library framework.

Purpose of the plugin

This plugin, together with the SignOn Library framework, allows client applications to access the user's certificates and keys stored in Cryptomathic Signer where certificates and keys are securely stored. This plugin enables this access through the SignOn Library Framework, so no direct access to Cryptomathic Signer is needed by the client application.

Quick-guide: Using the plugin

We assume that the reader has read the document "Using the SignOn library", and knows how to configure and call the SignOn method. Also the reader is assumed to have read "CAPI PKI Plugin Guide"; the Cryptomathic A/S Signer PKI plugin conforms to the same flow and differs only by the needed configuration settings, which will be described below.

```
// Application Context Settings for CrmSignerPkiPlugin
applicationContext.SetObject(SignerCtxKey.SignerHost, SIGNER_HOST;
applicationContext.SetObject(SignerCtxKey.SignerPort, SIGNER_PORT;
applicationContext.SetObject(SignerCtxKey.SignerAseExponent, SIGNER_ASE_EXP;
applicationContext.SetObject(SignerCtxKey.SignerAseModulus, SIGNER_ASE_MOD;
applicationContext.SetObject(SignerCtxKey.SignerCostumerDomain, SIGNER_CUST_DOMAIN;
```

- `SIGNER_HOST`:
  Alpha-numeric string specifying the host-name or IP-address of the machine hosting Cryptomathic Signer.
  Example: `10.0.0.145`
- `SIGNER_PORT`:
  Numeric string specifying the Customer Protocol port of Cryptomathic Signer. This normally 1992.
  Example: `1992`
- `SIGNER_ASE_EXP`:
  Hexadecimal string specifying the Cryptomathic Signer ASE key exponent. This value can be found by inspecting the ASE key file in a text-editor.
  Example: `010001`
- `SIGNER_ASE_MOD`:
  Hexadecimal string specifying the Cryptomathic Signer ASE key public modulus. This value can be found by inspecting the ASE key file in a text-editor.
  Example:
  `caf53eb1a137282c829335a30862163a5d9a65f4367b1473986403d34c0c949aef9005f9e1754a203b8ed164d0a6da57169865bd7db0fe3cb49d65fa673f992ea73d670a25cecab7ea077a39db9fb5db4f4612b3e118598fae90020a4fbb7215f2bc93c2c5cc6f58895d730f96efbbe0d5fb2765b9aca786799827aedd3fc2452ec603c312d52a16e40a732d3523dec82d173ab29ceee1c34fb8a84b9d77ee5dadd450d79277a564d135ff0bcb7a5801ddf40c3a82af8cdbb86a831c90ca833d`

- `SIGNER_CUST_DOMAIN:`
  Optional string representing the Signer customer domain. If the value is different from null and it is not an empty string the full username that is sent to Signer will be compound as follows: <SignerCtxKey.SignerCostumerDomain>-<username>